REMARKS

Reconsideration of the above-identified application in view of the amendments above and the remarks following is respectfully requested.

Claims 1-48 are in this Application, of which Claims 31-36 and 42 and have been withdrawn.

Claims 1-8, 11-20, 26, 30, 37-39, 41, and 43-47 were rejected under U.S.C. 102.

Claims 9-10, 21-25, 40, and 48 were rejected under U.S.C. 103.

Claim 1 has been amended herewith, to recite "protecting said datagram by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram; forwarding said protected datagram to said authentication server via the communication network, by said intermediate device, for authentication of the first user." Additionally, Claims 18, 21, and 24 have been amended to correct inadvertent errors appearing therein. It is submitted that no new matter has been added by these amendments, as they are purely cosmetic in nature.

Finally, new Claims 49-50 have been added, support for which may be found in the application, for example, as follows:

Claim 49 – page 15, line 3

Claim 50 – page 18, line 21; and page 24, line 1

35 U.S.C. § 102 Rejections

On page 3 of the Office Action, the Examiner has rejected Claims 1-8, 11-20, 26, 30, 37-39, 41, and 43-47 under 35 USC 102(b), as being anticipated by Caputo et al. (U.S. Patent No. 5,546,463). Applicants respectfully traverse this rejection.

In response, it is submitted that there is no prima facie basis for the Examiner's assertion that these claims are anticipated by the teachings of Caputo et al., as will be discussed below. In particular, Caputo et al. do not teach the limitations of amended Claim 1, which include "authenticating, using an authentication server, the use of an authentication device by at least a first user over a communication network via an intermediate communication device, comprising: receiving an interaction request with

said intermediate device by said intermediate device from said first user; responding to said interaction request by said intermediate device, to said first user; receiving an authentication datagram by said intermediate device, said authentication datagram including data from the first user, in response to said responding; protecting said datagram by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram; forwarding said protected datagram to said authentication server via the communication network, by said intermediate device, for authentication of the first user; and continuing interacting with said first user by said intermediate device in response to said authentication; wherein said intermediate device and said authentication server are separated from one another." Similarly, Caputo et al. do not teach the limitations of Claims 18, 19, and 26, as will be discussed below.

Caputo et al. teach a portable authentication device which can be carried by the user (column 4, line 24). The device includes a communications port for connection to a computer port of a personal computer, terminal, or telephone system (column 4, line 60). The device is authenticated, either by the presence of a secret/private key contained within the device or within a smartcard inserted into the device. Once authenticated, the device allows the user to gain access to a network, computer, or other protected communications facility (column 6, line 46). Optionally, user identification may also be performed, by the insertion of a PIN or password which uniquely identifies the person in possession of the device (column 6, line 56). Once the device authentication and, optionally, the user authentication procedure have been performed and succeed, then access to the network is enabled. No data may be transmitted until the authentication has been performed (column 8, line 29). After authentication, data is encrypted by the device before being transmitted via a telephone line to the network. The transmitted data is received, via a modem and decrypted before arriving at a destination computer/terminal (fig. 3, and column 8, line 10).

A first difference between the device to Caputo et al. and the invention as recited in the claims is that Caputo et al. do not teach transmitting data to an

authentication server over a network. Instead, the device to Caputo et al. performs local authentication of a device/user before data is transmitted to a network.

In contrast to Caputo et al., amended Claim 1 recites "A method of authenticating, using an authentication server, the use of an authentication device...over a communication network via an intermediate communication device, comprising...forwarding said datagram to said authentication server via the communication network, by said intermediate device, for authentication of the first user; and continuing interacting with said first user by said intermediate device in response to said authentication; wherein said intermediate device and said authentication server are separated from one another."

Additionally in contrast to Caputo et al., Claim 18 recites "A method of authentication of an authentication datagram by a remote authentication server, comprising: sending an encrypted datagram by secure computer communication from a vendor software to said remote authentication server, said encrypted datagram including data from the vendor; receiving said encrypted datagram by said remote authentication server...and outputting said binary validation answer for authentication of the vendor; wherein said vendor software and said remote authentication server are separated from one another."

Further in contrast to Caputo et al., Claim 19 recites "A method of authentication of an authentication datagram by a remote authentication server, comprising: sending an encrypted datagram by computer communication from an authentication device to said remote authentication server, said encrypted datagram including data from at least a first user; receiving said encrypted datagram by said remote authentication server...generating a validation answer by said remote authentication server, responsive to said search...wherein said authentication device and said remote authentication server are separated from one another."

Further in contrast to Caputo et al., Claim 26 recites "A method of remote validation of at least a first user, comprising: from the first user, receiving an authentication datagram by an authentication server from a remote authentication

device...for each datagram received, outputting a validation signal for the first user, in response to said corresponding counter value."

A second difference between the device to Caputo et al. and the invention as recited in the claims is that Caputo et al. teach encrypting data after authentication has been performed, as noted above. In contrast, amended Claim 1 recites "protecting said datagram by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram; forwarding said protected datagram to said authentication server via the communication network, by said intermediate device, for authentication of the first user."

Additionally in contrast to Caputo et al., Claim 18 recites "sending an encrypted datagram by secure computer communication from a vendor software to said remote authentication server...receiving said encrypted datagram by said remote authentication server...outputting said binary validation answer for authentication of the vendor."

Further in contrast to Caputo et al., Claim 19 recites "sending an encrypted datagram by computer communication from an authentication device to said remote authentication server, said encrypted datagram including data from at least a first user; receiving said encrypted datagram by said remote authentication server...generating a validation answer by said remote authentication server, responsive to said search...and outputting said validation answer for authentication of the first user."

Further in contrast to Caputo et al., Claim 26 recites "receiving an authentication datagram by an authentication server ...matching said datagram or a hash of said datagram to a corresponding table...calculating a corresponding counter value from a matching position in said corresponding table; and...if said authentication datagram is valid, increasing said corresponding counter over a previous counter,...and...outputting a validation signal for the first user, in response to said corresponding counter value."

In light of the above, it is submitted independent Claims 1, 18, 19, and 26 are not anticipated by Caputo et al. and are, therefore, allowable. It is further submitted that Claims (2-8, 11-17, 37, 43-47), (38), (20, 39), (30, 41) are allowable, as they depend from allowable independent Claims 1, 18, 19, and 26, respectively.

Claim Rejections – 35 U.S.C. § 103

On page 10 of the Office Action, Claims 9-10 , 24-25 were rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo et al. in view of Levi et al. (U.S. Patent No. 6,804,778). Applicant respectfully traverses this rejection.

Neither of the cited references teaches the limitations found in amended Claim 1, namely "authenticating, using an authentication server, the use of an authentication device...over a communication network via an intermediate communication device, comprising: receiving an interaction request with said intermediate device by said intermediate device from said first user; responding to said interaction...receiving an authentication datagram by said intermediate device...in response to said responding; protecting said datagram by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram; forwarding said protected datagram to said authentication server via the communication network, by said intermediate device, for authentication of the first user; and continuing interacting with said first user by said intermediate device in response to said authentication."

Additionally, neither of the cited references teaches the limitations found in Claim 24, namely "communication between a vendor and a user using an authentication device, comprising: generating a one time code for at least the user for a session by a card; receiving an authentication datagram from at least said user by an intermediate device of a vendor; forwarding said authentication datagram to a remote authentication server for authentication of the vendor when at least an indication of said one time code that matches the vendor is provided with said datagram; and forwarding said authentication datagram to said remote authentication server for authentication of the user when at least an indication of said one time code that matches said user is provided with said authentication datagram."

As noted above, Caputo et al do not teach transmitting data to an authentication server over a network, as recited in Claims 1 and 24, nor do they teach encrypting data after authentication has been performed, as recited in Claim 1.

Levi et al. teach a method of data quality assurance, wherein a request for data is received by a data provider over an Internet, data is received at the data provider, a quality assurance procedure is applied to the data, and the assured data is transmitted over the Internet. The reference does not teach "authenticating, using an authentication server, the use of an authentication device by at least a first user over a communication network via an intermediate communication device," as recited in Claim 1, nor does it teach "communication between a vendor and a user using an authentication device," as recited in Claim 24.

Additionally, it is submitted that even if one were inclined to combine the authentication device of Caputo et al. with the data quality assurance method to Levi et al, the resulting device would not include the limitations of Claims 1 and 24, noted above.

On page 11 of the Office Action, Claims 21-23, 40, and 48 were rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo et al. in view of Callais et al. (U.S. Patent No. 3,885,089) Applicant respectfully traverses this rejection.

Neither of the cited references teaches the limitations found in Claim 21, namely, "generating a code set for a remote authentication device, said remote authentication device configured for authentication of at least a first user comprising: providing a code generating software; providing at least one seed code for the first user for said software; generating said code set using said software and said seed; destroying said seed immediately after generating said code set; forwarding a first copy said code set to the first user; and storing a second copy said code set or an indication thereof on said remote authentication device; and authenticating the first user by matching between said first copy and said second copy or said indication thereof."

As noted above, Caputo et al do not teach transmitting data to an authentication server over a network, as recited in Claim 21.

Callais et al. teach a television scrambling system. They do not teach a method including a "remote authentication device configured for authentication of at least a first user," as recited in Claim 21.

Additionally, it is submitted that even if one were inclined to combine the authentication device of Caputo et al. with the television scrambling system of Callais et al, the resulting device would not include the limitations of Claim 21, noted above.

Applicant respectfully submits, therefore, that Claim 21 is patentable over Caputo et al. in view of Callais et al. It is further submitted that Claims 22-23, 40, and 48 are allowable, as they depend from allowable independent Claim 21.

In view of the foregoing remarks and amendments to the claims, reconsideration of the above-identified application, including Claims 1-30, 37-41, and 43-48 and new Claims 49-50, is respectfully requested.

Respectfully submitted,

/Jason H. Rosenblum/

Jason H. Rosenblum
Registration No. 56437
Telephone: 718.246.8482

Date: June 23, 2011